Global Information Assurance Certification Paper

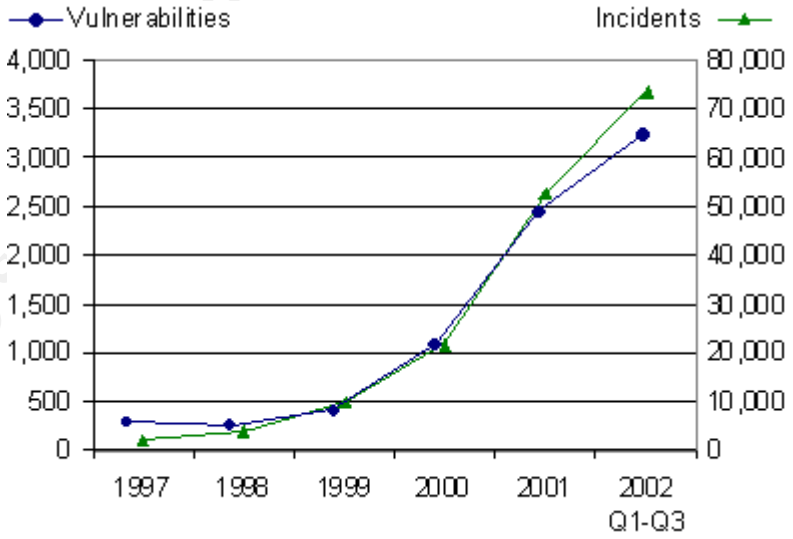
Certification for Systems Worthy of Trust

1. Abstract:

No one can be absolutely sure that a system will never have unauthorized entry, malicious code entered, a denial of service attack, catch a nasty virus, or be knocked out by a vicious act from man or nature. However, the best way to protect a system against the evils that lurk is to ensure that a system security certification and accreditation process is completed to make sure that the technical and non-technical controls are in place to mitigate known threats.

Network controls for many of today's government owned systems turn away thousands of unauthorized access attempts per minute, and after a review of router and firewall logs, many system administrators mistakenly believe that their systems are secure. After all, a system with no break-ins means a secure system right? – Wrong! No open system is 100% secure because an attacker only needs to find a single weakness in its defenses to breach the network and take control. Both internal and external sources provide relentless threats. Firewalls, IDS', and anti-virus controls alone no longer provide adequate protection for our information resources. Part of the problem is that the number of vulnerabilities and incidents has continued to grow at a near exponential rate since 1997. To add to this problem, there are system vulnerabilities that aren't even known about yet. But, with time they will surely become known as the Black Hats (hackers and the like), that keep one step ahead of us, continue their work.

Figure 1: Reported Security Vulnerabilities and Incidents (2)



Source: Cert, November 2002

From the graph in figure 1, it is clear that there is a direct relationship between the number of vulnerabilities and the number of incidents, and they both continue to grow (2). The question this raises is: What can be done to secure our digital assets? Simply said, all security vulnerabilities need to be identified, and secured. Although simple to say, there is no "silver bullet" that will eliminate all vulnerabilities, so there is no quick or easy way to eliminate the problem. But, by using the correct tools and approach, administrators can do a good job of protecting networks and the applications using them. Both process and technology need to be merged into a single, effective solution for security. If done correctly, systems can be certified as secure systems and worthy of trust. An added incentive to certify a system is to help system owners make an informed decision when authorizing a system to operate, which is a requirement identified in the Office of Management and Budget (OMB) Circular A-130 Appendix III (8).

In the following sections of this paper I will provide an overview for the process for certifying the security for a system. If followed, it will ensure that system security controls are implemented in such a way that a system can be operated in an environment worthy of trust. I will include in the discussion the method for completing the certification process with the use of a tool called *Xacta Web C&A*. First I will identify the requirements for certifying government systems. After identifying the requirements, I will discuss the certification process, and then discuss the Xacta tool and its role in certification of systems. I will then provide my conclusion. It should be noted that my discussion is focused on the Xacta tool, the tool's implementation requirements, user inputs, outputs, advantages, and disadvantages.

Although one hardly ever hears the word certification without the word accreditation following it (i.e. C&A), I will not discuss accreditation in detail because it is the end result and one of the reasons for certification. Also for the purpose of limiting the scope for this document, I will not discuss the different levels that could be identified for certification but instead proceed as if all systems are critical mission assets and need a high degree of certification. This discussion is also with the expectation that the enterprise already has an IT Security Policy, and knowledge of the Federal regulations and guidance for information security - prerequisites for the certification process.

2. Certification Requirements:

The government has gone from a manual method of doing business to a state of information technology (IT) reliance within a few relative years. Today, the government relies on IT to such a degree that if abruptly taken away, enterprises would crumble; IT comprises much of the critical information infrastructure within the United States.

As technology advances, systems become more and more complex to keep up with the growing ideas for automation and business benefit of increased productivity and service. The complexity of systems is a driving force for assessing the security using both technical and non-technical approaches. Information security must ensure

confidentiality, integrity, and availability to protect the privacy of the public, and at the same time ensure availability of the services that the users of the systems require. It's a fundamental management responsibility to ensure that the appropriate security controls are in place. Creating a living program to identify and mitigate risks will help system owners certify that a system is secure from theft, modification, and disruption or destruction of service. Most government agencies that are not part of DOD do not have classified information that pose a national threat if compromised. However, they do have sensitive information about the public and their own business processes that need to be protected.(6) It not only makes sense to protect this information and certify the security for systems, it's the law.

On December 17, 2002, President Bush signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA).(5) That signing made the requirements identified in the Government Information Security Reform Act of 2000 permanent. In effect, that permanently codified OMB Circular A-130 into law and made it a requirement for each government system be certified and accredited prior to implementation and at least every three years after that.(6)

3. The Certification Process:

The certification process is a comprehensive analysis of the technical and non-technical components of an IT system that needs to be completed before a system is moved into production.(6) Certification then needs to be completed again every three years or after a major change to the system.(8) The analysis needs to be completed in an operational environment to determine that the controls and system artifacts have been incorporated in compliance with Federal, Departmental, and other pertinent regulations or laws. Some examples of non-technical controls to be assessed are: system security documentation, physical security, personnel security, and risk management. Some examples of the technology that needs security certification are: Encryption devices/software, firewalls, access control, and audit tools.(3) This is only a partial list of items to think about. The system being certified needs a list that matches its own security configuration. Certification is a structured process that verifies techniques and procedures during the system's life cycle. It ensures that controls are implemented correctly and are effective to protect system confidentiality, integrity, and availability (CIA).

The certification process can be broken down into two main phases: Definition and Validation.

3.1 Definition phase:

In the definition phase you need to identify a certification team, develop a work plan, identify system boundaries, create a Security Evaluation and Test (ST&E) plan, and prepare an initial certification package. The certification package is called the System Security Authorization Agreement (SSAA)(7). The initial SSAA should be verified before starting validation and testing.

3.1.1 The Team: A team should be comprised of both management and technical representatives so that informed decisions can be made with the right technical advice. System users should also be represented so that the business process is not adversely affected. Once established, the team should meet initially to establish its roles within the team and also develop a certification work plan. The team should schedule regular meetings throughout the certification process to provide status on individual work assignments and make decisions on any open issues.

3.1.2 The Work Plan: The work plan should assign requirements that need to be completed along with a schedule that addresses the milestones relating to actions in each certification phase. The work plan should also identify cost estimates, and methods for accomplishing each task. Once completed, it should be kept as part of the SSAA and used as a baseline to determine status and whether the pending certification is being completed as scheduled.

3.1.3 System Boundaries: One of the most important steps in the certification process is to identify the system boundaries that are to be certified. This may not sound difficult, but with today's systems that have platform and network sharing, system interfaces and data exchanges, open system accesses, shared ownerships, dispersed locations, and centralized infrastructure support this task becomes very difficult. Help may come from the vulnerability scan parameters that have already defined, and there are other tools that will help find endpoints like the Xacta supported "Detect" software. However, many decisions have to be made first to define system boundaries. First off, think of what components a system owner has direct control over and the funding to support. For instance no one owns the Internet. What about the computers accessing it? Who controls the communication links between the interconnected systems? The list of concerns and areas to think about goes on, but this step should be thought out clearly before trying to certify resources that shouldn't be included, or miss some system components that should be included. If the system boundaries have already been identified in some system's security documentation, they should be validated in this phase.

3.1.4 ST&E Plan: At least as important as the definition of boundaries is the creation of the Security Test and Evaluation Plan. This is where it is determined what and how the controls on a system are going to be tested. To create a test plan, test scripts need to be created that are based on known vulnerabilities, security policy, federal security regulations and guidance, business requirements, system security plans and any other governing documentation related to the security of the system being certified. Also, if applicable, a selection of tools should be selected for penetration and vulnerability testing.

To assist in identifying known vulnerabilities to include in the test plan, information from previous audits and assessments should be reviewed. Also, advisories from sites like *FEDCIRC "Federal Computer Incident Response Center",* http://www.fedcirc.gov/ and *SANS/FBI Top 20 list* http://www.sans.org/top20/ should be referenced. The SANS top

20 list is an excellent source that identifies and explains the top 20 security vulnerabilities. It also provides information on port vulnerabilities that should be tested.(4)(9) Once completed, the ST&E plan should be included into the SSAA.

3.1.5 SSAA: The SSAA is a single repository for the activities created during the certification process and should include all security documentation for the system. The initial SSAA should include the C&A work plan, level of effort, cost estimates, roles and responsibilities, system descriptions and boundaries, and all related security documentation. Security documentation might include the system's security plan, completed risk assessment reports, contingency plans, configuration management plan, ST&E plan, and all current remediation plans for the system. The SSAA is a living document that will be updated throughout the certification process. However, before you can enter the validation phase, the artifacts within the SSAA need to be verified. (7)

3.2 Validation phase:

To avoid a conflict of interest, validation testing needs to be completed by an independent third party. During the validation phase, the ST&E plan will be carried out to include penetration testing and vulnerability scans if appropriate. Router and firewalls should be tested for open and unused ports and ports with known security vulnerabilities. Penetration testing will provide an assessment of the system's ability to undergo intentional attempts to compromise the system. Prior to scans and penetration testing, the rules of engagement need to be agreed to between those doing the testing, those operating the systems, and those who own the business process that the system supports. This is because, if not done properly, the test could inadvertently cause an interruption or degradation of service.

After the system has been tested, remediations may be necessary. From the results of the tests, a corrective action plan should be completed. The risks should be classified as low, medium, or high. To create a system worthy of trust, all high and medium risks should to be corrected before the system is certified. All other risks should be analyzed to determine what needs to be corrected and what the system owner wants to make a risk based decision not to correct. If the cost of repair outweighs the cost of the problem that could result if not mitigated, many system owners will elect not to repair the problem. This could be a mistake if public confidence is lost due to a problem occurring. It could conflict with the thought that the system is worthy of trust.

The independent third party should again validate all repairs. After all risks have been corrected to an acceptable level, the SSAA should be updated to include the results of the validation activity and the system should be certified secure for processing. The final SSAA should become the baseline security configuration document and be used during the next scheduled certification process.

4. Xacta Web C&A:

As identified in the certification process, probably the most difficult, time consuming, and expensive task is to create the ST&E plan. Especially if it has to be done for the hundreds of systems owned by most Federal Agencies. One enormous task for creating the ST&E plan is to determine what non-Agency regulations and guides need to be included for testing, and then what types of tests should be scripted from them.

An additional problem exists when storing the SSAA for so many systems, especially when the components in the SSAAs may be in different formats. The SSAA needs to be stored for future use -- According to Federal regulation; certification needs to be completed at least every three years for every system identified on an Agency's inventory.

What's the answer? Use a tool that already has test scripts for Federal regulation and guidance AND industry best practices already in it. Use a tool that will create a repository of SSAAs, in a standard format for future use. Use a tool that provides a standard, repeatable certification process. Those are the answers that Xacta's *Xacta Web C&A* tool provide.

Xacta Web C&A is the first COTS application that automates a major chunk of the security certification process. The tool reduces costs by creating a reusable and guided step-by-step process that has test scripts incorporated into it for federal regulations, standards, and best practices.

Another major hurdle in the certification process is the task of defining the system boundaries for the many systems to be certified. The manpower to collect this information is huge. The Xacta tool provides an answer for this also. An added benefit that comes along with the Xacta license is the use of Xacta's *Detect* tool that will map the actual system environment to help with boundary identification.(1)

It sounds joyous doesn't it? But before becoming overjoyed, it must be said that there are costs and work involved with using the tool. First a license has to be purchased to use the tool, training for users will be needed, and most of the activities identified in the

certification process still have to be completed as have identified in section 3. An implementation strategy will be needed for the tool and someone will need to be assigned to administer the tool. Those who administer the tool will need additional administrator training. Of course before using the tool, it needs to be secure. After all, the security for all of the systems using the tool will reside on its database, so it's data will be sensitive. It is therefore recommend that the system in which the tool resides be the first system certified -- before being populated with system SSAAs. Do not open this tool up to the public; only provide internal Intranet access.

4.1 Implementation:

From the *Xacta Web C&A Installation Guide*: "Xacta Web C&A is designed to run on the Microsoft Windows NT Server 4.0 and above with Service Pack 6a; Windows 2000 Server; Apache Web Server 1.3.19, or IIS Web Server 4.0 and above."

The minimum requirements as identified by Xacta for a high volume configuration are:(12)

SERVER SIDE
HOSTED CONFIGURATION
Web/Application Server*
• PIII 700 Processor
• 1 GB RAM
• 9 GB Hard Drive
Database Server*
• Dual PIII 700 Processor
• 1 GB RAM
• 9 GB Hard Drive
• Microsoft SQL Server 7.0 or above or Oracle 8.1.7
Publishing Server*
• Dual PIII 700 Processor
• 1 GB RAM
• 9 GB Hard Drive
• Microsoft Office 97 or above
* Note: Each of the computers listed above must have a minimum of one 10/100 Network Interface Card

CLIENT SIDE
• Computer with Netscape Communicator 4.73 or above or Internet Explorer 5.0 or above (free download) Major releases of new software will be supported within six months.
• Connected to an Ethernet network running TCP/IP
• Access to a printer
• Adobe Acrobat Reader 5.0

RECOMMENDED SKILL SETS
• NT Administration Skills
• Microsoft SQL/Oracle Server Administration Knowledge
• General Internet Knowledge (TCP/IP Networking)

An important part of the implementation is to ensure that the right hardware, database, and support software are configured properly before actually installing the Xacta software. It should be noted that for installation, the installer needs to log on as the NT Administrator. It should also be noted that during the install, the installation program will automatically install the necessary components for the Apache Web Server. The actual installation is easy with a screen-by-screen walkthrough with boxes to check and choices to make.(12)

4.2 User Inputs:

Before the Xacta tool can be used, the Agency specific content needs to be entered. As stated earlier, the tool gives a jump start by having federal regulations, standards, and best practices built in, but what about the Agency's or enterprise's security policy and guidance? That content also needs to be entered into the tool before the *Xacta Web C&A* system is ready for use. The key to selecting the correct enterprise content is whether or not it's testable. Only testable content should be added.

Another step that needs to be completed is that the content supplied with the tool needs to be evaluated. If not needed, the content needs to be deselected (i.e.: not many Agencies outside of DOD would need tempest tests). What remains combined with the Agency specific content entered, will create the Baseline Security Requirements for the Agency.

After the baseline has been created and the users have been provided access, it's time to start system specific work. The Agency's Baseline Security Requirements that have

already been established need to be reviewed again for applicability for each system (there's no need to test for encryption if the system doesn't use or need encryption). If a requirement isn't needed it can be deselected for that system's test. If a system has a unique security requirement that isn't covered in the baseline, it can be added. These actions should be completed by those most knowledgeable of the system being tested. They should be actions for the certification team identified during the certification process' definition phase.

After the system test criteria have been reviewed and approved, the SSAA (minus the ST&E plan) created during the definition phase should be entered into the tool.

4.3 Tool Output:

The tool will then create the ST&E plan as part of the SSAA. The SSAA package can be in the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP), the National Information Assurance Certification and Accreditation Process (NIACAP), or the Director of Central Intelligence Directive (DCID) formats.(11) For Agencies not part of DOD or the CIA, the NIACAP format should be used.

A NIACAP C&A process establishes the minimum standards for national security systems and provides information on the activities, tasks, and roles for completing C&A on systems to provide information assurance and the proper security posture. NIACAP is designed to complete the C&A process on an enterprise-wide view of systems relative to an Agency's mission and business processes. NIACAP is also designed to insure the proper level of security is maintained throughout the systems life cycle.(7)

One of the main reasons for selecting a specific C&A methodology like NIACAP is because the Xacta tool will provide its output in the format for that methodology. NIACAP identifies an SSAA document that describes the systems boundaries, documents test plans and procedures, test results and residual risk, security documentation, operating environment and threats, documents the C&A agreements, and forms the baseline security configuration document.(7) That's what most Agencies want in their SSAA.

Once the tool creates the SSAA, it should be given to an independent test group.

At this point the process is the same as the certification process' validation phase. However, validation should be easier when using the tool because the test plans will be standardized and easier for an independent source to complete testing. With certification of the system, the SSAA will remain in the repository for reference or access at any time. The SSAA is a living document and is a great beginning point for the next time certification is needed. In essence, by using the Xacta tool, a standardized, repeatable process has been created. Future use will require much less time and expense.

4.3 Advantages vs. Disadvantages:

Figure 2: Advantages and Disadvantages of using the Xacta Web C&A tool

Advantages	Disadvantages
Automatically generates hardware and software mapping with the Detect functionality	Requires licensing
Built-in content libraries for Federal regulations and best practices	Requires hardware and software
Creates automated test scripts	Creates new system that needs to be administered and maintained
Allows individual tailoring by system	Requires training
One button publishing with automated formatting for SSAAs	Requires a system administrator
Consistent SSAAs across all systems	New system needs certification for itself
Reusable content	
Reduced manpower costs in first year but has much higher cost benefits with future use	

Although the above chart shows the advantages and disadvantages of the Xacta tool, another column could have been included: disadvantages of not using the tool. Although they've already been discussed, the disadvantages of not using the tool may be somewhat obscure. The main disadvantages of not using the tool are: The information gathering for system boundaries including hardware and software information would need to be done manually, security libraries are scattered, no standardized format, manual effort needed to identify test criteria from Federal regulations and best practices, and processes could be lost and not reusable for required future certifications.(10)

5. Conclusion:

No system is 100% safe from internal and external evils. However, vulnerabilities and security incidents are increasing at an alarming rate and some measures have to be taken to ensure the controls on our systems adequately address the threat. One way to ensure controls are adequate is to complete a NIACAP certification and accreditation on systems to validate that the proper controls are implemented before a system is entered into production, and again every three years after that. The certification process is no easy task, enterprise wide it is a huge effort. Each step in the process needs to be planned carefully with system owners, technical support staff, and system users.

The certification process is completed in two main phases, the definition phase and the validation phase. In the definition phase, a certification team is identified, a work plan is developed, system boundaries are defined, an ST&E plan is created, and the initial SSAA is created. The SSAA is the binding certification document and will be updated throughout the process. In the validation phase, the SSAA is given to an independent review group to test the technical and non-technical security aspects of the system. When testing is complete, remediation needs to be completed on the risks found on the system. After all major risks have been mitigated and validated, the system can be certified.

Although the process sounds simple, the actions if done manually are very time consuming and do not create a standardized, reusable process. To help automate the process, Xacta markets a tool called *Xacta Web C&A*. The tool already has test scripts for federal regulations, standards, and best practices. It also assists in mapping system components for boundary definitions and creates a standardized, reusable SSAA in one of three formats. The NIACAP SSAA format is the one most non-DOD Agencies would select.

Although the tool provides a lot of benefit and decreases costs for certification in several areas, there are other costs associated with the tool. The tool needs to

become a system itself and requires certification. It also needs administration, training for users, and licensing.

The advantages for using the tool seem to outweigh the disadvantages for large multi-system Agencies. Future use of the tool provides additional cost savings because a repository of security information is kept for the next certification.

With or without the tool, the certification process identified in this paper is an approach that should be considered for providing information assurance and the proper security posture for systems worthy of trust.

References

1. A Hurwitz Group white paper written for: Xacta Corporation http://www.e-gov.gr/local/ism-egov/resources-ism/Proactive%20Enterprise%20Risk%20Management.pdf

2. Aberdeen Group, *Automated Vulnerability Remediation -- The Cure for Security's Common Cold*, http://www.aberdeen.com/2001/research/12023072.asp

3. Dr. Ron Ross, *Assessing the Security of Federal Information Systems,* http://csrc.nist.gov/sec-cert/ca-tutorial-bw.pdf

4. FEDCIRC, *The Federal Incident Response Center*, http://www.fedcirc.gov/

5. NIST, Computer Security Resource Center, *CSD news*, http://csrc.nist.gov/

6. NIST, *Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems*, http://csrc.nist.gov/sec-cert/SP-800-37-v1.0.pdf

7. NSTISSI No. 1000 April 2000, *National Information Assurance Certification and Accreditation Process (NIACAP),* http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf

8. Office of Management and Budget, *Circular No. A-130 Revised,* http://globalchange.gov/policies/a-130.html

9. SANS Institute, *SANS/FBI Top 20 List,* http://www.sans.org/top20/

10. Xacta, *Enabling Efficient, Consistent Certification and Accreditation Enterprise-Wide* http://www.acsac.org/2001/case/Thurs_C_1530_Berman_Xacta.pdf

11. Xacta, Products, *Xacta Web C&A,* http://www.xacta.com/products/webca/

12. Xacta, *Xacta Web C&A Installation Guide*